



UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office

Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. |
|-----------------|-------------|----------------------|---------------------|
| 09/059,765 | 04/14/98 | HIRATA | SONY-P8407 |

CHARLES P SAMMUT ESQ
LIMBACH LIMBACH LLP
2001 FERRY BUILDING
SAN FRANCISCO CA 94111

LMC1/0907

| |
|----------|
| EXAMINER |
|----------|

SEAL, J

| | |
|----------|--------------|
| ART UNIT | PAPER NUMBER |
|----------|--------------|

2766

DATE MAILED: 09/07/00

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

Art Unit: 2766

DETAILED ACTION

Specification

1. New Title approved and entered.
2. Minor changes to the specification on pages 2, 4, 5, 7, 18, 20, 32, 37, 43 have been entered and approved. Minor objections to the specification have been withdrawn.

Drawings

3. The application having been allowed, formal drawings are required in response to this Office action.
4. Prior art objection to Figure 1, is maintained. Applicant is asked to point out what is novel or new in Figure 1?

Claim Rejections - 35 USC § 103

5. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.
6. Claims 1-9 remain rejected under 35 U. S. C. 103 as being anticipated by Lawrence Berardinis (August 1996) and further in view of Schneier (1995) as previously applied and as addressed below.

Art Unit: 2766

7. In claim 1 applicant recites a remote controlled receiving apparatus transmitting through a network which transmits encrypted certification information to a processor (apparatus has a means extracting, decrypting and storing control commands) to control an electronic device.

8. In his article Appliance On-line, Berardines teaches about washer, dryers, air conditioning and refrigerators getting on the information superhighway (ie the Internet, page 72). Linked by digital networks, these intelligent objects will form what Hawley (machine Design, March 1995)"the global, digital fabric" (page 73, column 1). Besides setting their own clocks, tomorrow's appliances will perform other mundane chores like paying the utility bills, scheduling repairs, and ordering food, detergent, and household necessities from online cybermarkets. (Page 73, column 1). By the year 2000, 22% of all Internet-access devices will be machines other than CP's. This is sure to include smart household appliances. (Page 78, column

2). Berardines does not mention the use of E-mail as the particular link of the appliances with the outside world, but he does say that house owner will have over-ride capability (page 78, column 2). Examiner note that control messages that would enable appliances to interlink with the cybermarket or in turn for the homeowner to over-ride pre-existing commands and institute new commands would have to be by E-mail or ftp, and because of the ease, E-mail would be the user-friendly choice.

9. Berardines is also silent on the use of cryptology in his article, but Schneier (Applied Cryptology) teaches the application of cryptology to communication such as the Internet. One of average skill in the art of remote control or telemetry, would be aware of the problems of sending

Art Unit: 2766

instructions over the Internet to one's house to control certain appliances. As has recently been made so very obvious, the Internet is susceptible to many different attacks by hackers and other malicious people. Thus encryption would be a prudent precaution. Claim 1 is rejected.

10. In claim 2, applicant recites an apparatus with the limitations of claim 1 and further with a means for executing control commands stored in memory of the receiving apparatus.

11. Berardinis does not specifically mention executing control commands stored in memory, but if a homeowner suddenly needs to change his mind and have dinner served for 16 instead of 5, appropriate commands would need to be stored in memory to make such a system user-friendly. Claim 2 is rejected.

12. In claim 3-4, applicant recites a method with the limitations of claim 1 with the further limitations that the predetermined user information is used to authentication user which is encrypted/decryption by secrete key, first extracts authentication information and then control information and finally decrypting control information if authentication is verified.

13. Predetermined user information to authenticate user for access to resources is well known in the art. For example a password in a computer account. Information sent could be sent in both secret or public key cryptology (these are standard in the art see Schneier, Applied Cryptography). Exacting the authentication before extracting the commands is usually what is done in authentication system, if for no other reason to save CPU time. Decryption of the command information after authentication would then follow. Claims 3-4 are rejected.

Art Unit: 2766

14. In claim 5, applicant recites a method for implementing the apparatus of claim 1. It therefore contains the same limitations with respect to art as claim 1 and is therefore claim 5 is rejected.

15. In claim 6, applicant recites a transmitting apparatus with a means of encryption of the control commands and the predetermined certification information, an inputting this information as an electronic signal (such as E-mail) on to a network (such as the Internet).

16. Berardinis teaches a communication link consisting of a transmitter and receiver (a PC or more likely some other type of smaller more compact device to the Internet). The discussion of encryption/decryption authentication have been addressed above. Claim 6 is rejected in view of the same prior art.

17. In claim 7, applicant recites a method for implementing the apparatus of claim 6. It therefore contains the same limitations with respect to art as claim 1 and is therefore rejected maintained.

18. In claim 8, applicant recites a device consisting of a transmitter and receiver such that their is an encryption part in the transmitter, which can encrypt commands and certification transmit this information over a network to a receiver which extracts the commands and certification information, stores the commands and decrypts the certification comparing it with stored information to designated user.

Art Unit: 2766

19. The use of transmitting and receiving devices and encryption/decryption for interfacing with the Internet, is well known in the art and defines a communication system. Claim 8 is rejected on the same prior art as used above.

20. In claim 9, applicant recites a methods implementation of claim 8. It therefore contains the same limitations with respect to art as claim 1 and is therefore claim 9 is rejected.

Response to Remarks

21. DA is silent as to how the electronic control commands, from a browser gets to the actual device being programed, however from DA's Internet embodiment, the means available for transmitting such information is limited to E-mail and ftp. Ftp would be good for batches of such commands, but for an individual programing his VCR from his office E-mail would be the easiest and most straightforward methods of the two choices.

22. The need for securing E-mail, e-commerce, personal, financial and medical records, business records to mention but a few is well recognized in the art. In Bruce Schneier E-Mail Security, How to Keep Your Electronic Messages Private (1995), Chapter 1, is devoted to the need for E-mail security. He points out with the fact that with the Internet a decentralized system, any and everyone can intercept and read mail (pages 6-9 point out possible eavesdropping). Further the number of "Viruses" implemented by E-mail in the last decade and the proliferation of companies that make anti virus programs for E-mail illustrate that E-mail security is a legitimate concern of people using E-mail on the Internet for whatever reason. As

Art Unit: 2766

pointed out in the examiner's previous action, there are a number of good reason for encrypting control signals over an E-mail link. The most obvious, in addition to those discussed by Schneier are intentional and unintentional jamming of commands. One for example launch a denial of service attack on a person using the E-mail to control his VCR for example or one could attach viruses to such E-mails. Such tampering could prove very destructive if instead of the VCR it was an oven being controlled as such. So Schneier does teach E-mail security in general and in this specific case of remote control those in the art of remote control (such as model planes and boats) using interference free telemetry.

23. DA teaches the use of electronic control signals to operate devices (e.g. a VCR) remotely via the Internet (one embodiment) and as previously argued, those skilled in the art would use Internet E-mail to do this, via a computer and an Internet browser with hyperlink like facilities to associate program labels (eg The Simpson's) with on-screen icons such as *record this* (page 276 lines 20-23). Even though DA suggest only TV and radio (page 276, line 19) or VCR (page 276, line 12), it would be obvious to anyone skilled in the art of remote control, that the teachings of DA could be extended to control most any home appliance.

24. If an appliance is to be preprogrammed, there must be memory to store those control commands. In the event of a VCR, the device itself has memory and a timer, but in the case of a radio also mentioned by DA such devices seldom have memory and hence implies there must be memory onboard the controller. Also it would be more efficiency to store such information (control commands) at the appliance end, so as not to tie up the Internet or phone lines.

Art Unit: 2766

25. Encryption of a predetermined text such as a password such as at a terminal, sending such a password to a mainframe, and then decrypting it and comparing it to one stored on a machine, is one of the first means of computer security on a mainframes. One has two choices as far as encryption of the predetermined material (say the password), either public key or secret key cryptographic methods. Both are discussed at length in Schneier. The motivation for E-mail security is discussed above.

References Cited But Not Applied

26. In addition to the art disclosed above, the examiner would also like to mention art which pertain but not applied.

27. The use of remote control via encrypted communication links is at least as old as the patent issued to Hedy Kiesler Markey (Hedy Lamarr) and George Antheil Secret Communication System in August 1941 (2292387). This patent is important for a number of reasons. It was the first application of remote control of an electronic device (a steerable torpedo) over an encrypted communication link (so that the control commands are secure) and the first application of spread spectrum communications (to prevent jamming). The Markey et al. patent contains the elements of a user interface, network (radio network), encryption, and controlled device (torpedo). Even though different technology is used the same ideas are involved.

28. Kobayashi (JP 7322371) teaches the remote control of household appliances (television, VCR, air condition using) a by using a digital cordless phone connected to data equipment by a transmission line (see Figure 1) such as a personal computer remotely by radio waves.

Art Unit: 2766

29. Another patent Ugajin, US 5652892 July 1997, describes a method of controlling remote power sources (an electrical device) with a check of user ID (authentication) and password control over a network (e.g. Internet) with security.

30. Patent EP917052 Remotely Controlling Device Over Internet uses a lab top to control devices A ... N remotely from over the Internet (see figure 1).

31. Patent JP 9781034, Toshiaki et. al. (Mar 97), points to the use of a controller operating a plurality of electric household appliance operated in communication with an external host. The household appliances (19 Figure 1) are connected to a server (11 Figure 1) through the Internet 3 which receives information from an external server (7). Again illustrating the heart of the applicant's invention. These patents are listed to show an unbroken link in remote control technology leading to the development of remotely controlled devices using the latest network, the Internet.

32. Disclosed Anonymously (henceforth DA, May 1996) teaches a device that uses an interface with the Internet, a web page with an electronic program guide and VPS or PDC codes for identifying programs, and hypertext labels with icons such as "record this" to allow a multimedia station to reproduce or record radio or television programs remotely by means of a simple point-and-click operation. The use of hypertext commands does not restrict invention, as all electrical devices need a start time and a run time. DA teaches all aspects of the appliance invention with the exception of encryption of transmitted signals (DA is silent on that teaching) and user authentication. Schneier teaches various means for encrypting a signal including

Art Unit: 2766

classical (chapter 1) public key (chapter 19) and symmetric key (DES chapter 12) encryption/decryption and further teaches the use of authentication (pages 52-56). The motivation to substitute secure communications encompassed by the teaching of Schneier for the clear communication taught by DA amounts to the prevention of unauthorized changes in the multimedia programming (or other electronic devices) either unintentional or intentional. Such changes could be minor such as missing a TV program because someone changed the scheduling on the VCR or very serious, if the device remotely controlled is a power grid.

33. Finally the examiner would like to note that the idea of the control of house hold objects by computers and the Internet date back to the 50s. In his 1950 stories "There Will Come Soft Rains" science fiction author tell of a tale of computerized houses of the future. Also Thomas Pynchon, in the early 1950's discusses a global communication net in which all peoples would be interconnected (see Thomas Pynchon, Hero of Cyberspace). Someone of average skill in the art would have been able to have combined the teaches of Pynchon and Bradbury to obtain a smart home interconnected to the Internet.

Conclusion

34. Any inquiry concerning this communication should be direct to James Seal at telephone number (703) 308 4562. The examiner can normally be reached on Monday through Friday from 7:30 a.m. to 5:30 p.m.

Art Unit: 2766

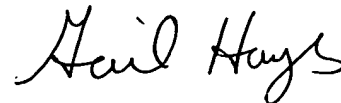
35. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gail Hayes, can be reached at (703) 305-9711.

36. Any inquiry of a general nature or relating to the status of this application or preceding should be directed to the Group receptionist, whose telephone number is (703) 305-3800. Fax number is (703) 305 0040.

James Seal



21 August 2000



GAIL O. HAYES
SUPERVISORY PATENT EXAMINER
GROUP 2700